Issues with PAD/SPD and BTNS

draft-ietf-btns-core

Nico Williams <Nicolas.Williams@sun.com>
Michael Richardson <mcr@xelerance.com>

Assumptions

- security gateway in host-based VPN mode (either no hosts behind gateway, or hosts are NAT'ed, even inside tunnel).
- has large number of remote sites, that connect from a static IP, with a certificate based authentication, which includes subjectAltName, giving IP address.

mcr@xelerance.co

Assumptions (2)

- policy (SPD and PAD) are configured to accept any host with a certificate from a pre-configured CA, with the right subjectAltName.
  - (canonically, this includes a mythical global-PKI).
- too many sites to have explicit PAD/SPD entries.
- policy includes some special behaviour for hosts that are authenticated (important part)

mcr@xelerance.co

Still with me?

- now is a good time to make sure you understand the situation
- microphone please

mcr@xelerance.co

Add in BTNS

a BTNS node may assert a single IP address, in transport and/or tunnel/32 (BEET-like only) mode.

☞ a BTNS node may therefore assert an IP address which is also in the PKI.

☞ a BTNS node may impersonate a node from the site-to-site PKI-authenticated VPN

(note assumes that BTNS can pass three-way handshake, so it is true for all people on wireless in this room)

mcr@xelerance.co

What breaks?

- the nodes behind the BTNS node (if NAT) and/or the BTNS node itself may send packets to the wrong host.
- real world example:
  - large SMTP based intranet,
  - DNS (primary + secondary communication)
  - other large distributed system

mcr@xelerance.co

Characterizing the problem

- Multiple “wildcard” PAD entries such that for a peer can assert the same TSs whether it matches one wildcard PAD entry or the other
  - and where for some of those traffic selectors applications assume IPsec authenticates peers

mcr@xelerance.co

How to fix this (1)

- "Doctor it hurts when I lift my arm"
  - "Don't lift your arm"
  - caution against this situation
- Advise not to enable BTNS in this situation.
  - Or restrict BTNS to port TSs for apps where this is OK

Unfortunately, for some systems BTNS may be seem as a transitional mechanism towards a real PKI

mcr@xelerance.co

How to fix this (2)

- put all special hosts into SPD
- expose BTNS status to applications that care via API

➔ make “special part” depend upon having used the right certificate (and chain)

mcr@xelerance.co

Conclusions

- this is a problem that is really hard to get into by accident.
- needs to be written up in security considerations.
- it can be avoided/worked around.

mcr@xelerance.co

How to explain this in security considerations?

- please give advice on this
- open mike

mcr@xelerance.co